INFS 767
Secure Electronic Commerce
Fall 1999

Lecture 2
RBAC

Prof. Ravi Sandhu

DAC/MAC/RBAC

- Owner-based discretionary access control (DAC)
  - Origins: academia
- Mandatory access control (MAC)
  - Origins: military
    - lattice-based access control (LBAC)
    - Bell-LaPadula (BLP) model
- Role based access control (RBAC)
  - Origins: business

2

CAUTION

- There is more to access control than
  - owner based DAC
  - MAC/LBAC/BLP
  - RBAC
- Generalized access control models
  - HRU, Take-Grant, SPM, TAM
  - Type enforcement
  - Generalized framework for access control

OWNER-BASED DAC

- owner has all-or-nothing power
  - superuser fallacy
- spaghetti of intent
- negative permissions make for messier spaghetti
- trojan horses can subvert intent

MAC/LBAC/BLP

- enforce one-directional information flow in a lattice of security labels
- can be used for
  - confidentiality
  - integrity
  - aggregation (Chinese Wall)
  - combinations of these

5

IMPASSE

STRONG? WEAK?		WEAK? STRONG?
Owner Based DAC	⟷	MAC/LBAC/BLP
chaotic anarchic useless		rigid simple-minded useless

6

RBAC

- A user's permissions are determined by the user's roles rather than
  - user's identity (DAC)
  - user's clearance (MAC)
- Facilitates
  - administration of permissions
  - articulation of policy

7

RBAC

- Policy neutral
- Policy oriented
  - least privilege
  - separation of duties
  - encapsulation of primitive permissions
  - separation of administration and access
  - Roles are a semantic construct around which to build policy

8

RBAC vs GENERALIZED ACCESS CONTROL MODELS

- **Generalized access control models can be configured to do RBAC**

  <u>but</u>
- **do not provide convenient means for this purpose**

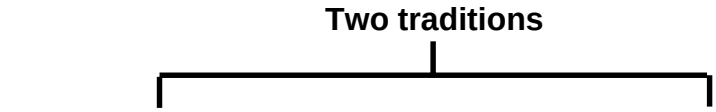
9

RBAC vs GENERALIZED ACCESS CONTROL MODELS

- **RBAC is**
  - **policy neutral**
  - **policy oriented**
- **General access control models are**
  - **policy neutral**
  - **mechanism oriented**

10

RBAC



Support system-wide administrative functions

Programmed into individual applications

11

RBAC

- **Often used to separate administrative functions**
  - **Operator**
  - **Auditor**
  - **Security Officer**
  - **User**

12

RBAC: WHAT'S NEW

- **Extend system support into application domain**
- **Use RBAC to manage RBAC**

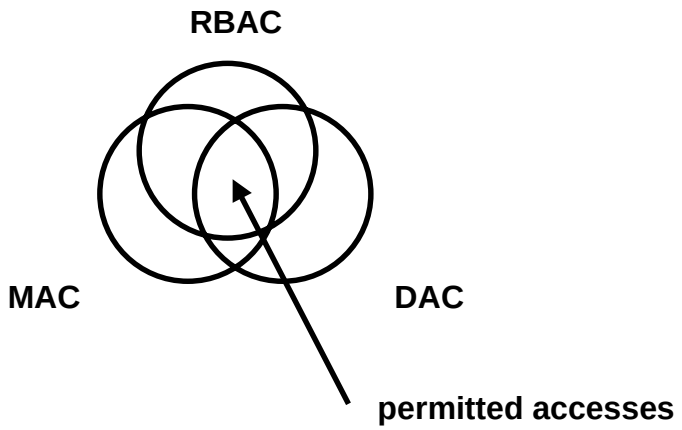
13

WHAT IS THE POLICY IN RBAC?

- **RBAC is a framework to help in articulating policy**
- **The main point of RBAC is to facilitate security management**

14

INTERACTION OF RBAC, MAC AND DAC



15

WHAT IS RBAC?

- **multidimensional**
- **open ended**
- **ranges from simple to sophisticated**

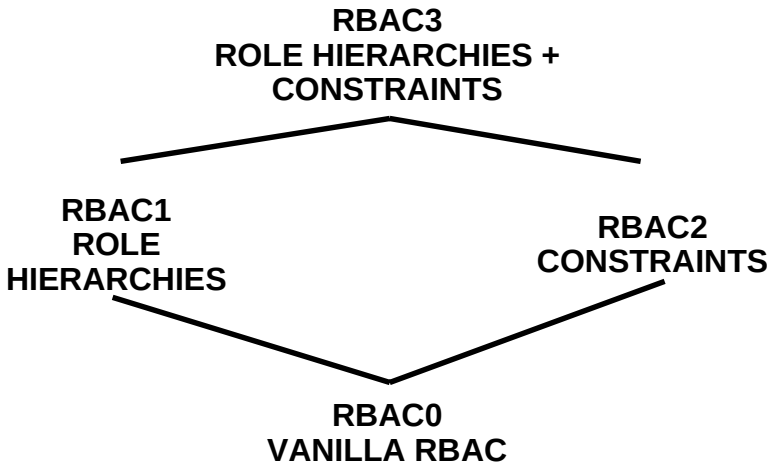
16

RBAC CONUNDRUM

- turn on all roles all the time
- turn on one role only at a time
- turn on a user-specified subset of roles

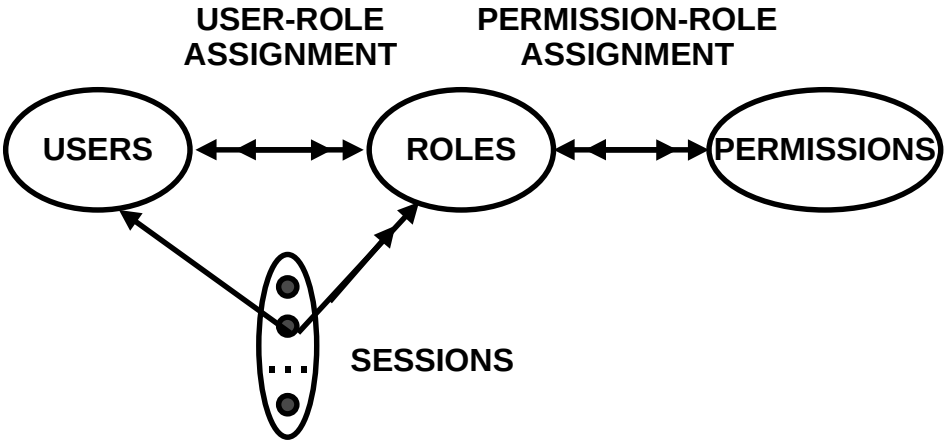
17

RBAC96 FAMILY



18

RBAC0



19

PERMISSIONS

- **Primitive permissions**
  - **read, write, append, execute**
- **Abstract permissions**
  - **credit, debit, inquiry**

20

PERMISSIONS

- System permissions
  - auditorObject permissions
  - read, write, append, execute, credit, debit, inquiry

21

PERMISSIONS

- Permissions are positive
- No negative permissions or denials
  - negative permissions and denials can be handled by constraints
- No duties or obligations
  - outside scope of access control

22

ROLES AS POLICY

- A role brings together
  - a collection of users and
  - a collection of permissions
- These collections will vary over time
  - A role has significance and meaning beyond the particular users and permissions brought together at any moment

23

ROLES VERSUS GROUPS

- Groups are often defined as
  - a collection of users
- A role is
  - a collection of users and
  - a collection of permissions
- Some authors define role as
  - a collection of permissions

24

USERS

- Users are
  - human beings or
  - other active agents
- Each individual should be known as exactly one user

25

USER-ROLE ASSIGNMENT

- A user can be a member of many roles
- Each role can have many users as members

26

SESSIONS

- A user can invoke multiple sessions
- In each session a user can invoke any subset of roles that the user is a member of

27

PERMISSION-ROLE ASSIGNMENT

- A permission can be assigned to many roles
- Each role can have many permissions

28

MANAGEMENT OF RBAC

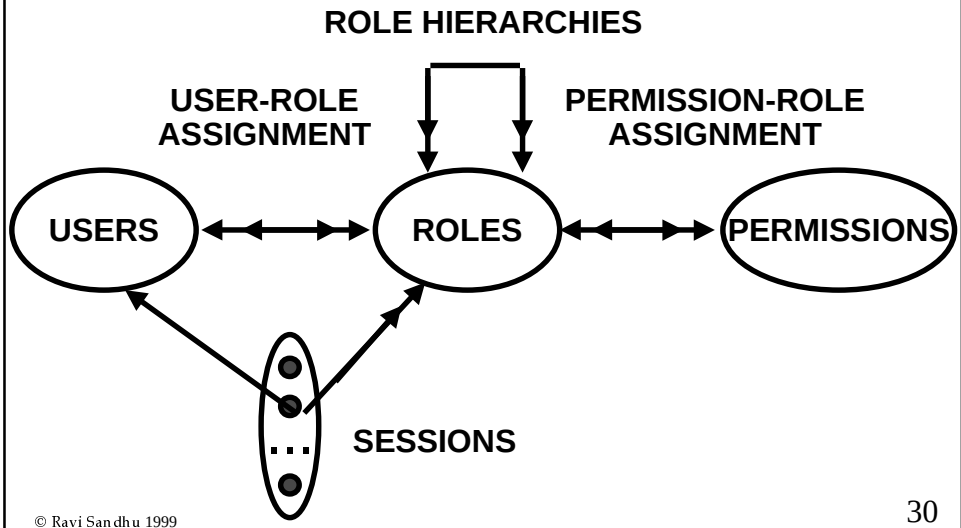
- **Option 1:**

  USER-ROLE-ASSIGNMENT and PERMISSION-ROLE ASSIGNMENT can be changed only by the chief security officer
- **Option 2:**

  Use RBAC to manage RBAC

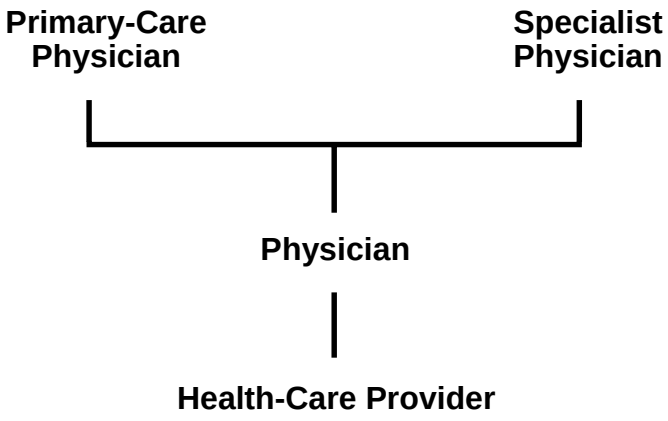
29

RBAC1



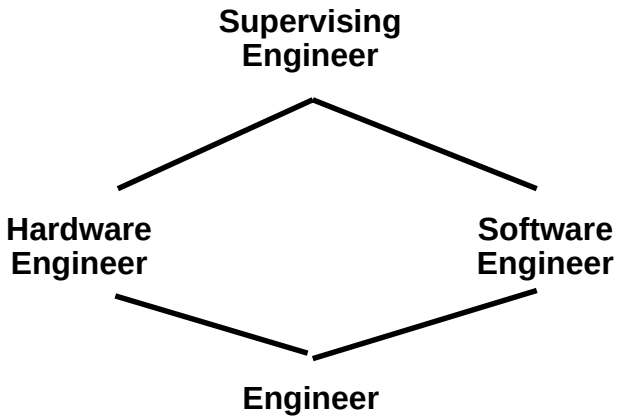
30

HIERARCHICAL ROLES



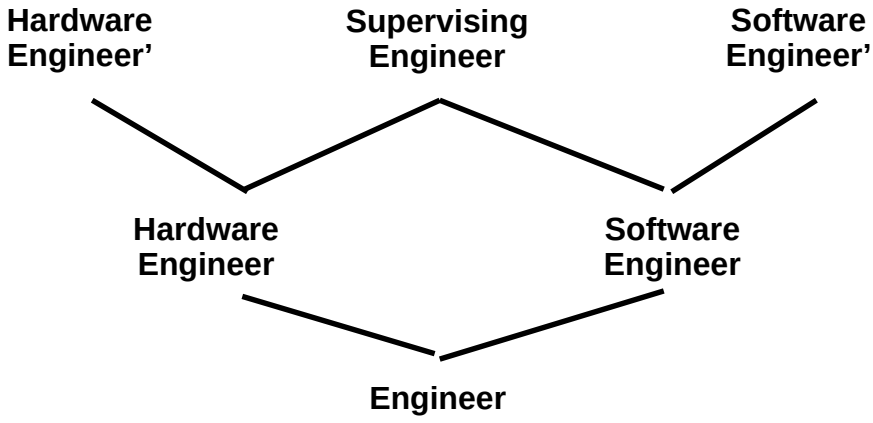
31

HIERARCHICAL ROLES



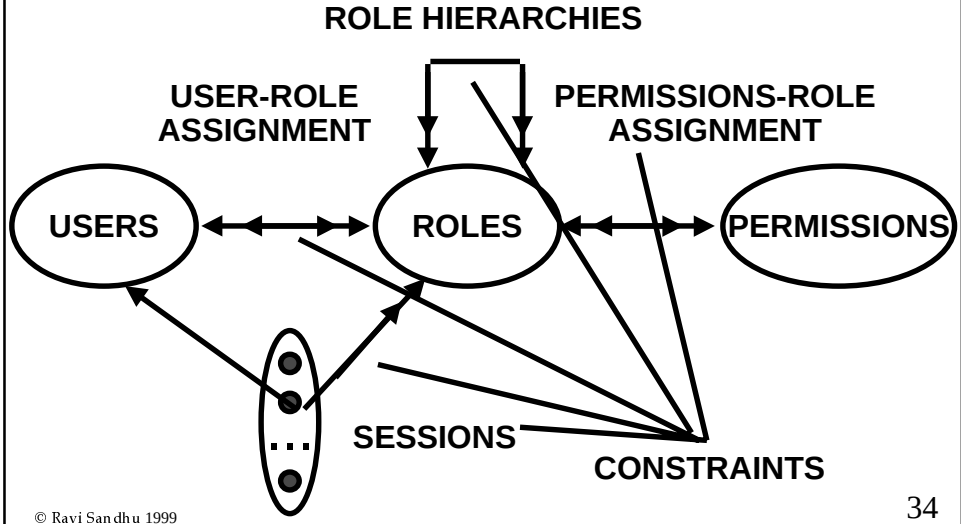
32

PRIVATE ROLES



33

RBAC: R3



34

CONSTRAINTS

- **Mutually Exclusive Roles**
  - **Static Exclusion: The same individual can never hold both roles**
  - **Dynamic Exclusion: The same individual can never hold both roles in the same context**

35

CONSTRAINTS

- **Mutually Exclusive Permissions**
  - **Static Exclusion: The same role should never be assigned both permissions**
  - **Dynamic Exclusion: The same role can never hold both permissions in the same context**

36

CONSTRAINTS

- **Cardinality Constraints on User-Role Assignment**
  - **At most k users can belong to the role**
  - **At least k users must belong to the role**
  - **Exactly k users must belong to the role**

37

CONSTRAINTS

- **Cardinality Constraints on Permissions-Role Assignment**
  - **At most k roles can get the permission**
  - **At least k roles must get the permission**
  - **Exactly k roles must get the permission**

38

SCALE AND RATE OF CHANGE

- Hundreds of roles
- Thousands of users
- Frequent changes to
  - user-role assignment
  - permission-role assignment
- Less frequent changes for
  - role hierarchy

39